



Athens Authentication Point

Recognized as:

U.S. Patent & Trademark
Office, Scientific & Technical
(665-54-532)

US Patent and Trademark
2007 3686.002
(911-40-100)

Welcome!

To use the personalized
features of this site, please
log in or **register**.

If you have forgotten your
username or password, we
can **help**.

My SpringerLink

Marked Items

Alerts

Order History

Saved Items

All

Favorites

**Content Types Subject Collections****Data Encryption**

REMOVE Search For (Boolean) > (homomorphism OR
homomorphic) AND (abelian OR commutative) AND (signature OR
hashing OR hash)
REMOVE Subject > Data Encryption

Disable Highlighting

Expanded View**Condensed View**182 Results First | 1-10 | **11-20** | 21-30 | 31-40 | 41-50 | Next

- ☒ Access to all content ☒ Access to some content
☐ Access to no content

- ☐ **11.** Journal Article Add to marked items
The Round Functions of
Cryptosystem PGM Generate the
Symmetric Group

DOI 10.1007/s10623-005-5667-z
Journal Designs, Codes and
Cryptography
Issue Volume 38, Number 1 /
January, 2006
Authors A. Caranti and F. Dalla. Volta
Subject Collection Mathematics and Statistics
Abstract ...et al. have described
symmetric and public key
cryptosystems based on
logarithmic signatures (also
known as group bases) for
finite permutation groups
Text PDF (103 kb)
Rightslink Permissions & Reprints

- ☐ **12.** Journal Article Add to marked items
A General Zero-
Knowledge Scheme

DOI 10.1023/A:1008237708202
Journal Designs, Codes and
Cryptography
Issue Volume 12, Number 1 /
September, 1997
Authors Mike Burmester, Yvo G.
Desmedt, Fred Piper and
Michael Walker
Subject Collection Mathematics and Statistics
Text PDF (5 kb)
Rightslink Permissions & Reprints

- ☐ **13.** Journal Article Add to marked items
Identity-based key

Find

(homomorp

☒ Within i☐ Within t**Starts With**

a b c d e

p q r s t

SpringerL

In the last

In the last

In the last

Content T

Book Chap

Journal Art

Subject

Computer

Computer

Networks (

Artificial In

Robotics) (

Software E

Database f

Algorithm

Complexity

Computati

(171)

Mathemati

Combinato

Data Struc

Informatio




Copyright


2007 (27)

2006 (31)

2005 (46)

- | | | |
|------------------------------|---|--|
| | agreement protocols from pairings | 2004 (40) |
| | Category Regular Contribution | 2003 (4) |
| | DOI 10.1007/s10207-006-0011-9 | 2000 (12) |
| | Journal International Journal of Information Security | 1999 (4) |
| | Issue Volume 6, Number 4 / July, 2007 | 1998 (8) |
| | Authors L. Chen, Z. Cheng and N. P. Smart | 1997 (10) |
| | Subject Collection Computer Science | Publicatio |
| | Text PDF (534 kb) HTML | Lecture No Science (1 |
| | Rightslink Permissions & Reprints | Designs, C (9) |
| <input type="checkbox"/> 14. | Book Chapter A Useful Undecidable Theory | Add to marked items Internation Informatio |
| | DOI 10.1007/978-3-540-73001-9_73 | Author |
| | Book Series Lecture Notes in Computer Science | José Meseg |
| | Volume Volume 4497/2007 | Ivan Damg |
| | Book Computation and Logic in the Real World | Serge Vaur |
| | Author Victor L. Selivanov | Stéphanie |
| | Subject Collection Computer Science | Ronald Cra |
| | Text PDF (395 kb) | Hartmut El |
| <input type="checkbox"/> 15. | Book Chapter Functorial Semantics of Rewrite Theories | Add to marked items Huaxiong \ |
| | Category Algebraic Specification and Logic | Paliath Nar |
| | Book Series Lecture Notes in Computer Science | Franz Baac |
| | Volume Volume 3393/2005 | Alfred Men |
| | Book Formal Methods in Software and Systems Modeling | |
| | Author José Meseguer | |
| | Subject Collection Computer Science | |
| | Text PDF (222 kb) | |
| <input type="checkbox"/> 16. | Book Chapter Weak Fields for ECC | Add to marked items |
| | Category Elliptic Curve Cryptosystems | |
| | Book Series Lecture Notes in Computer Science | |
| | Volume Volume 2964/2004 | |
| | Book Topics in Cryptology - CT-RSA 2004 | |
| | Authors Alfred Menezes, Edlyn Teske and Annegret Weng | |
| | Subject Collection Computer Science | |

	Text	PDF (300 kb)	HTML
 17.	Book Chapter Petri nets, process algebras and concurrent programming languages	Add to marked items	
	Category	IV Applications of Elementary Net Systems and Place/Transition Nets	
	DOI	10.1007/3-540-65307-4_46	
	Book Series	Lecture Notes in Computer Science	
	Volume	Volume 1492/1998	
	Book	Lectures on Petri Nets II: Applications	
	Authors	Eike Best, Raymond Devillers and Maciej Koutny	
	Subject Collection	Computer Science	
	Text	PDF (5,397 kb)	
 18.	Book Chapter Analysis of a Multi-party Fair Exchange Protocol and Formal Proof of Correctness in the Strand Space Model	Add to marked items	
	Category	Exchanges and Contracts	
	DOI	10.1007/11507840_23	
	Book Series	Lecture Notes in Computer Science	
	Volume	Volume 3570/2005	
	Book	Financial Cryptography and Data Security	
	Authors	Aybek Mukhamedov, Steve Kremer and Eike Ritter	
	Subject Collection	Computer Science	
	Text	PDF (224 kb)	
 19.	Book Chapter Verifiable Shuffle of Large Size Ciphertexts	Add to marked items	
	DOI	10.1007/978-3-540-71677- 8_25	
	Book Series	Lecture Notes in Computer Science	
	Volume	Volume 4450/2007	
	Book	Public Key Cryptography – PKC 2007	
	Authors	Jens Groth and Steve Lu	
	Subject Collection	Computer Science	
	Abstract	...correctness of a shuffle. We first suggest a HVZK argument based on homomorphic integer commitments, and improve both on round	

		complexity, communication complexity and computational...
	Text	PDF (541 kb)
	20. Book Chapter	Add to marked items
	Algorithms to Speed Up Computations in Threshold RSA	
	Category	Secret Sharing II
	DOI	10.1007/10718964_36
	Book Series	Lecture Notes in Computer Science
	Volume	Volume 1841/2000
	Book	Information Security and Privacy
	Author	Brian King
	Subject Collection	Computer Science
	Abstract	...Frankel described a threshold scheme which can be used with any finite abelian group. Hence it can be used to provide a threshold RSA scheme...
	Text	PDF (243 kb)

182 Results First | 1-10 | **11-20** | 21-30 | 31-40 | 41-50 | Next

Frequently asked questions | General information on journals and books | Send
Impressum

© Springer. Part of Springer Science+Business Media

Privacy, Disclaimer, Terms and Conditions, © Copyright Information

Remote Address: 151.207.242.4 • Server: mpweb20

HTTP User Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; InfoPath.1; .NET CLR 2.0.50727)



Content Types Subject Collections

Athens Authentication Point

Recognized as:

U.S. Patent & Trademark
Office, Scientific & Technical
(665-54-532)

US Patent and Trademark
2007 3686.002
(911-40-100)

Welcome!

To use the personalized
features of this site, please
log in or **register**.

If you have forgotten your
username or password, we
can **help**.

My SpringerLink

Marked Items

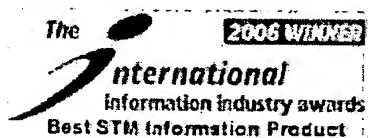
Alerts

Order History

Saved Items

All

Favorites



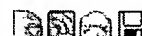
Data Encryption

REMOVE Search For (Boolean) > "group
homomorphism" AND (signature OR hash OR hashing)
REMOVE Subject > Data Encryption

Disable Highlighting

Expanded View

Condensed View



37 Results First | **1-10** | 11-20 | 21-30 | 31-37 | Next

- ☒ Access to all content
☒ Access to some content
☐ Access to no content

<input type="checkbox"/> 1.	Book Chapter	Add to marked items
	On Pairing	
	Inversion Problems	
	DOI	10.1007/978-3-540-73489-5_18
	Book Series	Lecture Notes in Computer Science
	Volume	Volume 4575/2007
	Book	Pairing-Based Cryptography – Pairing 2007
	Author	Takakazu Satoh
	Subject Collection	Computer Science
	Text	PDF (453 kb)

<input type="checkbox"/> 2.	Book Chapter	Add to marked items
	Efficient Zero-	
	Knowledge Proofs of Knowledge	
	without Intractability Assumptions	
	Book Series	Lecture Notes in Computer Science
	Volume	Volume 1751/2004
	Book	Public Key Cryptography
	Authors	Ronald Cramer, Ivan Damgård and Philip MacKenzie
	Subject Collection	Computer Science
	Text	PDF (354 kb)

<input type="checkbox"/> 3.	Book Chapter	Add to marked items
	Cryptographic	
	Asynchronous Multi-party	
	Computation with Optimal	
	Resilience (Extended Abstract)	
	Category	Secure Protocols

Find

"group homomorphism"

☒ Within all content☐ Within these results

Starts With

a b c d e f g h i j
p q r s t u v w x y

SpringerLink Date

In the last six months

In the last year (9)

Content Type

Book Chapters (35)

Journal Articles (2)

Subject

Computer Science (3)

Computer Communication
Networks (36)Artificial Intelligence
Robotics (35)Software Engineering
Database ManagementAlgorithm Analysis and
Complexity (35)Computation by Abstract
(35)

Mathematics (1)

Management of Computer
Information SystemsData Structures, Cryptography
Information Theory

Copyright

2007 (6)

2006 (4)

2005 (10)

2004 (10)

- | | | | |
|--|--------------------|--|---|
| | DOI | 10.1007/11426639_19 | 2000 (1) |
| | Book Series | Lecture Notes in Computer Science | 1999 (1) |
| | Volume | Volume 3494/2005 | 1998 (5) |
| | Book | Advances in Cryptology – EUROCRYPT 2005 | Publication |
| | Authors | Martin Hirt, Jesper Buus Nielsen and Bartosz Przydatek | Lecture Notes in Computer Science (35) |
| | Subject Collection | Computer Science | Designs, Codes and (1) |
| | Text | PDF (277 kb) | International Journal of Information Security |
- ☐ 4. Book Chapter Add to marked items
- Cryptanalysis of Two Anonymous Buyer-Seller Watermarking Protocols and an Improvement for True Anonymity**
- | | | |
|-------------|---|--------------------|
| Category | Cryptographic Protocols | Author |
| Book Series | Lecture Notes in Computer Science | Tsuyoshi Takagi |
| Volume | Volume 3089/2004 | Serge Vaudenay |
| Book | Applied Cryptography and Network Security | Jean Monnerat |
| Authors | Bok-Min Goi, Raphael C.-W. Phan, Yanjiang Yang, Feng Bao, Robert H. Deng and M.U. Siddiqi | Ronald Cramer |
| | | Ivan Damgård |
| | | Feng Bao |
| | | Maurice Herlihy |
| | | Takakazu Satoh |
| | | Katja Schmidt-Samr |
| | | Sergio Rajsbaum |
-
- ☐ 5. Book Chapter Add to marked items
- Homomorphic Cryptosystems Based on Subgroup Membership Problems**
- | | |
|--------------------|---------------------------------------|
| Category | Homomorphic Encryption |
| DOI | 10.1007/11554868_22 |
| Book Series | Lecture Notes in Computer Science |
| Volume | Volume 3715/2005 |
| Book | Progress in Cryptology – Mycrypt 2005 |
| Author | Kristian Gjosteen |
| Subject Collection | Computer Science |
| Text | PDF (219 kb) |
-
- ☐ 6. Book Chapter Add to marked items
- Efficient Strongly Universal and Optimally Universal**

- | | | |
|--|--------------------|---|
| | Hashing | |
| | Extended Abstract | |
| | DOI | 10.1007/3-540-48340-3_24 |
| | Book Series | Lecture Notes in Computer Science |
| | Volume | Volume 1672/1999 |
| | Book | Mathematical Foundations of Computer Science 1999 |
| | Author | Philipp Woelfel |
| | Subject Collection | Computer Science |
| | Abstract | New hash families are analyzed, mainly consisting of the hash functions $h_{a,b}$... |
| | Text | PDF (594 kb) |
-
- ☐ 7. Book Chapter Add to marked items
- Cryptanalysis of Two Non-anonymous Buyer-Seller Watermarking Protocols for Content Protection
- | | |
|--------------------|---|
| DOI | 10.1007/978-3-540-74472-6_77 |
| Book Series | Lecture Notes in Computer Science |
| Volume | Volume 4705/2007 |
| Book | Computational Science and Its Applications - ICCSA 2007 |
| Authors | Bok-Min Goi, Raphael C. -W. Phan and Hean-Teik Chuah |
| Subject Collection | Computer Science |
| Text | PDF (442 kb) |
-
- ☐ 8. Book Chapter Add to marked items
- Reducing Logarithms in Totally Non-maximal Imaginary Quadratic Orders to Logarithms in Finite Fields
- | | |
|-------------|---------------------------------------|
| Category | Integers and Computation |
| Book Series | Lecture Notes in Computer Science |
| Volume | Volume 1716/2004 |
| Book | Advances in Cryptology - ASIACRYPT'99 |

	Authors	Detlef Hühnlein and Tsuyoshi Takagi
	Subject Collection	Computer Science
	Text	PDF (220 kb)
<input type="checkbox"/> 9.	Book Chapter Efficient Private Matching and Set Intersection	Add to marked items
	Book Series	Lecture Notes in Computer Science
	Volume	Volume 3027/2004
	Book	Advances in Cryptology - EUROCRYPT 2004
	Authors	Michael J. Freedman, Kobbi Nissim and Benny Pinkas
	Subject Collection	Computer Science
	Abstract	...We present protocols, based on the use of homomorphic encryption and balanced hashing, for both semi-honest and malicious environments. For lists of length k ...
	Text	PDF (326 kb)
<input type="checkbox"/> 10.	Book Chapter Cryptography, Connections, Cocycles and Crystals: A p-Adic Exploration of the Discrete Logarithm Problem	Add to marked items
	Category	Public Key Cryptanalysis
	Book Series	Lecture Notes in Computer Science
	Volume	Volume 3348/2004
	Book	Progress in Cryptology - INDOCRYPT 2004
	Authors	H. Gopalkrishna Gadiyar, K. M. Sangeeta Maini and R. Padma
	Subject Collection	Computer Science
	Text	PDF (147 kb)

37 Results First | **1-10** | 11-20 | 21-30 | 31-37 | Next

Frequently asked questions | General information on journals and books | Send feedback | Impressum

© Springer. Part of Springer Science+Business Media

Privacy, Disclaimer, Terms and Conditions, © Copyright Information

Remote Address: 151.207.242.4 • Server: mpweb04

HTTP User Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; InfoPath.1; .NET CLR 2.0.50727)



Athens Authentication Point

Recognized as:

U.S. Patent & Trademark
Office, Scientific & Technical
(665-54-532)

US Patent and Trademark
2007 3686.002
(911-40-100)

Welcome!

To use the personalized
features of this site, please
log in or **register**.

If you have forgotten your
username or password, we
can **help**.

My SpringerLink

Marked Items
Alerts
Order History

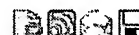
Saved Items

All
Favorites

**Content Types Subject Collections****Data Encryption**

REMOVE Search For (Boolean) > "group homomorphism"
AND (signature OR hash OR hashing)
REMOVE Subject > Data Encryption

Disable Highlighting

Expanded View**Condensed View**37 Results First | 1-10 | **11-20** | 21-30 | 31-37 | Next

- ☐ Access to all content
☒ Access to some content
☐ Access to no content

- ☐ **11.** Journal Article Add to marked items
The Round
Functions of Cryptosystem PGM
Generate the Symmetric Group

DOI 10.1007/s10623-005-5667-z
Journal Designs, Codes and Cryptography
Issue Volume 38, Number 1 / January, 2006
Authors A. Caranti and F. Dalla Volta
Subject Collection Mathematics and Statistics
Abstract ...et al. have described symmetric and public key cryptosystems based on logarithmic signatures (also known as group bases) for finite permutation groups
Text PDF (103 kb)
Rightslink Permissions & Reprints

- ☐ **12.** Journal Article Add to marked items
Identity-based key
agreement protocols from pairings

Category Regular Contribution
DOI 10.1007/s10207-006-0011-9
Journal International Journal of Information Security
Issue Volume 6, Number 4 / July, 2007

Find

"group homomorphism"

- ☒ Within all content
☐ Within these results

Starts With

a b c d e f g h i
p q r s t u v w x

SpringerLink Date

In the last six months
In the last year (9)

Content Type

Book Chapters (35)
Journal Articles (2)

Subject

Computer Science (1)
Computer Communications Networks (36)
Artificial Intelligence Robotics (35)
Software Engineering
Database Management
Algorithm Analysis and Complexity (35)
Computation by Abstraction (35)
Mathematics (1)



Management of Confidential Information Systems
Data Structures, Cryptography and Information Theory

Copyright

2007 (6)
2006 (4)
2005 (10)
2004 (10)

	Authors	L. Chen, Z. Cheng and N. P. Smart	2000 (1)
	Subject Collection	Computer Science	1999 (1)
	Text	PDF (534 kb) HTML	1998 (5)
	Rightslink	Permissions & Reprints	Publication
<input type="checkbox"/> 13.	Book Chapter	Add to marked items	Lecture Notes in Computer Science (35)
	Two-Party Privacy-Preserving Agglomerative Document Clustering		Designs, Codes and (1)
	DOI	10.1007/978-3-540-72163-5_16	International Journal of Information Security
	Book Series	Lecture Notes in Computer Science	Author
	Volume	Volume 4464/2007	Tsuyoshi Takagi
	Book	Information Security Practice and Experience	Serge Vaudenay
	Authors	Chunhua Su, Jianying Zhou, Feng Bao, Tsuyoshi Takagi and Kouichi Sakurai	Jean Monnerat
	Subject Collection	Computer Science	Ronald Cramer
	Text	PDF (412 kb)	Ivan Damgård
			Feng Bao
			Maurice Herlihy
			Takakazu Satoh
<input type="checkbox"/> 14.	Book Chapter	Add to marked items	Katja Schmidt-Samra
	Weak Fields for ECC		Sergio Rajsbaum
	Category	Elliptic Curve Cryptosystems	
	Book Series	Lecture Notes in Computer Science	
	Volume	Volume 2964/2004	
	Book	Topics in Cryptology - CT-RSA 2004	
	Authors	Alfred Menezes, Edlyn Teske and Annegret Weng	
	Subject Collection	Computer Science	
	Text	PDF (300 kb) HTML	
<input type="checkbox"/> 15.	Book Chapter	Add to marked items	
	Generic Homomorphic Undeniable Signatures		
	Category	Digital Signatures	
	Book Series	Lecture Notes in Computer Science	
	Volume	Volume 3329/2004	
	Book	Advances in Cryptology - ASIACRYPT 2004	
	Authors	Jean Monnerat and	

- | | | |
|--|--------------------|--|
| | Subject Collection | Serge Vaudenay |
| | Abstract | Computer Science |
| | | ...that we transform a private group homomorphism from public groups G...being public) into an undeniable signature scheme. It is provably secure... |
| | Text | PDF (241 kb) |
-
- ☒ **16.** Book Chapter Add to marked items
Custodian-Hiding Verifiable Encryption
- | | |
|--------------------|---|
| Category | Public Key Schemes I |
| Book Series | Lecture Notes in Computer Science |
| Volume | Volume 3325/2005 |
| Book | Information Security Applications |
| Authors | Joseph K. Liu, Victor K. Wei and Duncan S. Wong |
| Subject Collection | Computer Science |
| Text | PDF (208 kb) |
-
- ☒ **17.** Book Chapter Add to marked items
Pairing-Friendly Elliptic Curves of Prime Order
- | | |
|--------------------|--|
| Category | Efficient Implementations |
| DOI | 10.1007/11693383_22 |
| Book Series | Lecture Notes in Computer Science |
| Volume | Volume 3897/2006 |
| Book | Selected Areas in Cryptography |
| Authors | Paulo S.L.M. Barreto and Michael Naehrig |
| Subject Collection | Computer Science |
| Text | PDF (450 kb) |
-
- ☐ **18.** Book Chapter Add to marked items
Factorization-Based Fail-Stop Signatures Revisited.
- | | |
|-------------|---|
| Book Series | Lecture Notes in Computer Science |
| Volume | Volume 3269/2004 |
| Book | Information and Communications Security |

- | | |
|--------------------|---|
| Author | Katja Schmidt-Samoa |
| Subject Collection | Computer Science |
| Abstract | Fail-stop signature (FSS) schemes are important primitives because in a fail-stop signature scheme... |
| Text | PDF (2,137 kb) |
-  **19.** Book Chapter Add to marked items
Paillier's
Cryptosystem Modulo $p^2 q$ and Its
Applications to Trapdoor
Commitment Schemes
- | | |
|--------------------|--|
| Category | Homomorphic Encryption |
| DOI | 10.1007/11554868_21 |
| Book Series | Lecture Notes in Computer Science |
| Volume | Volume 3715/2005 |
| Book | Progress in Cryptology – Mycrypt 2005 |
| Authors | Katja Schmidt-Samoa and Tsuyoshi Takagi |
| Subject Collection | Computer Science |
| Abstract | ...Tauman on-line/off-line signatures.
Keywords:
homomorphic encryption, trapdoor commitments, trapdoor hash families, on-line/off-line... |
| Text | PDF (287 kb) |
-
-  **20.** Book Chapter Add to marked items
Fast Bilinear Maps
from the Tate-Lichtenbaum Pairing
on Hyperelliptic Curves
- | | |
|--------------------|--|
| Category | Curves over Finite Fields and Applications |
| DOI | 10.1007/11792086_33 |
| Book Series | Lecture Notes in Computer Science |
| Volume | Volume 4076/2006 |
| Book | Algorithmic Number Theory |
| Authors | Gerhard Frey and Tanja Lange |
| Subject Collection | Computer Science |
| Abstract | ...also as a building block for |

cryptosystems with
special properties like
short signatures or
identity based
encryption. In this
paper we consider the
Tate pairing...

Text

PDF (485 kb)

37 Results First | 1-10 | **11-20** | 21-30 | 31-37 | Next

Frequently asked questions | General information on journals and books | Send
feedback | Impressum

© Springer. Part of Springer Science+Business Media

Privacy, Disclaimer, Terms and Conditions, © Copyright Information

Remote Address: 151.207.242.4 • Server: mpweb19

HTTP User Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; InfoPath.1; .NET CLR 2.0.50



Athens Authentication Point

Recognized as:

U.S. Patent & Trademark
Office, Scientific & Technical
(665-54-532)

US Patent and Trademark
2007 3686.002
(911-40-100)

Welcome!

To use the personalized
features of this site, please
log in or **register**.

If you have forgotten your
username or password, we
can **help**.

My SpringerLink

Marked Items

Alerts

Order History

Saved Items

All

Favorites

**Content Types Subject Collections****Data Encryption**

REMOVE Search For (Boolean) > "group homomorphism"
AND (signature OR hash OR hashing)
REMOVE Subject > Data Encryption

Disable Highlighting

Expanded View**Condensed View**37 Results First | 1-10 | 11-20 | **21-30** | 31-37 | Next

- ☒ Access to all content
☒ Access to some content
☐ Access to no content

- 21.** Book Chapter Add to marked items
A wait-free
classification of loop agreement
tasks

Extended abstract

Category

DOI

Book Series

Volume

Book

Authors

Subject Collection

Abstract

Contributed Papers

10.1007/BFb0056482

Lecture Notes in
Computer Science

Volume 1499/1998

Distributed

Computing

Maurice Herlihy and
Sergio Rajsbaum

Computer Science

...can be assigned an
algebraic signature
consisting of a
finitely-
presented...only if
there exists a group
homomorphism $\Phi: G$
 $\rightarrow H$ carrying...

PDF (757 kb)

Text

- 22.** Book Chapter Add to marked items
Undeniable
Signatures Based on Characters:
How to Sign with One Bit

Book Series

Volume

Book

Authors

Lecture Notes in
Computer Science

Volume 2947/2004

Public Key
Cryptography - PKC
2004Jean Monnerat and
Serge Vaudenay**Find**

"group homomorphism"

☒ Within all content☐ Within these results**Starts With**

a b c d e f g h i
p q r s t u v w x

SpringerLink Date

In the last six months

In the last year (9)

Content Type

Book Chapters (35)

Journal Articles (2)

Subject

Computer Science (1)

Computer Commun-
Networks (36)Artificial Intelligence
Robotics (35)

Software Engineerin

Database Managemen

Algorithm Analysis a
Complexity (35)Computation by Abs
(35)

Mathematics (1)




Management of Corr
Information SystemData Structures, Cry
Information Theory**Copyright**



2007 (6)

2006 (4)

2005 (10)

2004 (10)

	Subject Collection	Computer Science	2000 (1)
	Abstract	We present a new undeniable signature scheme which is based on the computation of characters. Our signature scheme...	1999 (1) 1998 (5)
	Text	PDF (306 kb) HTML	Publication Lecture Notes in Computer Science (35) Designs, Codes and (1)
	23. Book Chapter Implementing Cryptographic Pairings over Barreto-Naehrig Curves	Add to marked items	International Journal of Information Security
	DOI	10.1007/978-3-540-73489-5_10	Author Tsuyoshi Takagi
	Book Series	Lecture Notes in Computer Science	Serge Vaudenay
	Volume	Volume 4575/2007	Jean Monnerat
	Book	Pairing-Based Cryptography – Pairing 2007	Ronald Cramer Ivan Damgård
	Authors	Augusto Jun Devegili, Michael Scott and Ricardo Dahab	Feng Bao Maurice Herlihy Takakazu Satoh
	Subject Collection	Computer Science	Katja Schmidt-Sam
	Text	PDF (422 kb)	Sergio Rajsbaum
	24. Book Chapter Overview of elliptic curve cryptography	Add to marked items	
	DOI	10.1007/BFb0054012	
	Book Series	Lecture Notes in Computer Science	
	Volume	Volume 1431/1998	
	Book	Public Key Cryptography	
	Authors	Kiyomichi Araki, Takakazu Satoh and Shinji Miura	
	Subject Collection	Computer Science	
	Text	PDF (1,205 kb)	
	25. Book Chapter A Wait-Free Classification of Loop Agreement Tasks (Extended Abstract)	Add to marked items	
	Book Series	Lecture Notes in Computer Science	
	Volume	Volume 1499/1998	
	Book	Distributed Computing	

	Authors	Maurice Herlihy and Sergio Rajsbaum
	Subject Collection	Computer Science
	Abstract	...can be assigned an algebraic signature consisting of a finitely-presented...only if there exists a group homomorphism $\phi : G \rightarrow H$...
	Text	PDF (570 kb)
 26.	Book Chapter Optimization of the MOVA Undeniable Signature Scheme	Add to marked items
	Category	Implementation Issues
	DOI	10.1007/11554868_14
	Book Series	Lecture Notes in Computer Science
	Volume	Volume 3715/2005
	Book	Progress in Cryptology - Mycrypt 2005
	Authors	Jean Monnerat, Yvonne Anne Oswald and Serge Vaudenay
	Subject Collection	Computer Science
	Abstract	...results on the MOVA undeniable signature scheme presented last year by...is based on a secret group homomorphism. The original MOVA scheme...
	Text	PDF (240 kb)
 27.	Book Chapter A New Cramer-Shoup Like Methodology for Group Based Provably Secure Encryption Schemes	Add to marked items
	Category	Encryption and Signatures
	Book Series	Lecture Notes in Computer Science
	Volume	Volume 3378/2005
	Book	Theory of Cryptography
	Authors	Maria Isabel González Vasco, Consuelo Martínez, Rainer Steinwandt

- | | | |
|--|--------------------|---------------------|
| | Subject Collection | and Jorge L. Villar |
| | Text | Computer Science |
| | | PDF (219 kb) |
-
- ☐ **28.** Book Chapter Add to marked items
Zero-knowledge
proofs for finite field arithmetic, or:
Can zero-knowledge be for free?
- | | |
|--------------------|---|
| DOI | 10.1007/BFb0055745 |
| Book Series | Lecture Notes in
Computer Science |
| Volume | Volume 1462/1998 |
| Book | Advances in
Cryptology —
CRYPTO '98 |
| Authors | Ronald Cramer and
Ivan Damgård |
| Subject Collection | Computer Science |
| Text | PDF (1,132 kb) |
-
- ☐ **29.** Book Chapter Add to marked items
2 RSA and
Probabilistic Prime Number Tests
- | | |
|--------------------|---|
| Book Series | Lecture Notes in
Computer Science |
| Volume | Volume 3028/2004 |
| Book | Probabilistic and
Statistical Methods in
Cryptology |
| Author | Daniel
Neuenschwander |
| Subject Collection | Computer Science |
| Text | PDF (274 kb) |
-
- ☐ **30.** Book Chapter Add to marked items
Pairings on Elliptic
Curves over Finite Commutative
Rings
- | | |
|--------------------|---|
| Category | Number Theoretic
Foundations |
| DOI | 10.1007/11586821_26 |
| Book Series | Lecture Notes in
Computer Science |
| Volume | Volume 3796/2005 |
| Book | Cryptography and
Coding |
| Authors | Steven D. Galbraith
and James F. McKee |
| Subject Collection | Computer Science |
| Text | PDF (265 kb) |

37 Results First | 1-10 | 11-20 | **21-30** | 31-37 | Next

Frequently asked questions | General information on journals and books | Send

[feedback](#) | [Impressum](#)

© Springer. Part of Springer Science+Business Media

[Privacy](#), [Disclaimer](#), [Terms and Conditions](#), © [Copyright Information](#)

Remote Address: 151.207.242.4 • Server: mpweb22

HTTP User Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; InfoPath.1; .NET CLR 2.0.50727)



Athens Authentication Point

Recognized as:

U.S. Patent & Trademark
Office, Scientific & Technical
(665-54-532)

US Patent and Trademark
2007 3686.002
(911-40-100)

Welcome!

To use the personalized
features of this site, please
log in or register.

If you have forgotten your
username or password, we
can **help.**

My SpringerLink

Marked Items

Alerts

Order History

Saved Items

All

Favorites

**Content Types Subject Collections****Data Encryption**

REMOVE Search For (Boolean) > "group homomorphism"
AND (signature OR hash OR hashing)
REMOVE Subject > Data Encryption

Disable Highlighting

Expanded View**Condensed View**37 Results First | 1-10 | 11-20 | 21-30 | **31-37** | Next

- ☐ Access to all content
☒ Access to some content
☐ Access to no content

- ☐ **31.** Book Chapter Add to marked items
Upper Bounds on
the Communication Complexity of
Optimally Resilient Cryptographic
Multiparty Computation

Category Multiparty
Computation
DOI 10.1007/11593447_5
Book Series Lecture Notes in
Computer Science
Volume 3788/2005
Book Advances in
Cryptology -
ASIACRYPT 2005
Authors Martin Hirt and
Jesper Buus Nielsen
Subject Collection Computer Science
Text PDF (301 kb)

- ☐ **32.** Book Chapter Add to marked items
On Multiplicative
Secret Sharing Schemes

Category Secret Sharing I
DOI 10.1007/10718964_28
Book Series Lecture Notes in
Computer Science
Volume 1841/2000
Book Information Security
and Privacy
Authors Huaxiong Wang, Kwok
Yan Lam, Guo-Zhen
Xiao and Huanhui
Zhao
Subject Collection Computer Science
Abstract ...such as in threshold
RSA signature
schemes. In this paper

Find

"group homomorphism"

☒ Within all content☐ Within these results**Starts With**

a b c d e f g h i
p q r s t u v w x

SpringerLink Date

In the last six months

In the last year (9)

Content Type

Book Chapters (35)

Journal Articles (2)

Subject

Computer Science (1)

Computer Communi-
Networks (36)Artificial Intelligence
Robotics (35)

Software Engineerin

Database Managemen

Algorithm Analysis a
Complexity (35)Computation by Abs
(35)

Mathematics (1)

Management of Corr
Information System:Data Structures, Cry
Information Theory**Copyright**

2007 (6)

2006 (4)

2005 (10)

2004 (10)



- | | | | |
|--|------|---|----------------------------------|
| | | we...a notion of multiple perfect hash families, which we introduce in... | 2000 (1)
1999 (1)
1998 (5) |
| | Text | PDF (142 kb) | |
-
- ☐ **33.** Book Chapter Add to marked items
Optimistic fair exchange of digital signatures
 Extended abstract
 DOI 10.1007/BFb0054156
 Book Series Lecture Notes in Computer Science
 Volume Volume 1403/1998
 Book Advances in Cryptology — EUROCRYPT'98
 Authors N. Asokan, Victor Shoup and Michael Waidner
 Subject Collection Computer Science
 Abstract We present a new protocol that allows two players to exchange digital signatures over the Internet in a fair way, so that either each player...
- | | | |
|--|------|--------------|
| | Text | PDF (895 kb) |
|--|------|--------------|
-
- ☐ **34.** Book Chapter Add to marked items
Efficient Proofs of Knowledge of Discrete Logarithms and Representations in Groups with Hidden Order
 Category Building Blocks
 Book Series Lecture Notes in Computer Science
 Volume Volume 3386/2005
 Book Public Key Cryptography - PKC 2005
 Authors Endre Bangerter, Jan Camenisch and Ueli Maurer
 Subject Collection Computer Science
 Text PDF (272 kb)
-
- ☐ **35.** Book Chapter Add to marked items
Do All Elliptic Curves of the Same Order Have the Same Difficulty of Discrete Log?

Publication

Lecture Notes in Computer Science (35)
 Designs, Codes and Cryptography (1)
 International Journal of Information Security

Author

Tsuyoshi Takagi
 Serge Vaudenay
 Jean Monnerat
 Ronald Cramer
 Ivan Damgård
 Feng Bao
 Maurice Herlihy
 Takakazu Satoh
 Katja Schmidt-Sammler
 Sergio Rajsbaum

Category	Algebra and Number Theory
DOI	10.1007/11593447_2
Book Series	Lecture Notes in Computer Science
Volume	Volume 3788/2005
Book	Advances in Cryptology - ASIACRYPT 2005
Authors	David Jao, Stephen D. Miller and Ramarathnam Venkatesan
Subject Collection	Computer Science
Text	PDF (562 kb)
<hr/>	
 36.	Book Chapter Definability in the Homomorphic Quasiorder of Finite Labeled Forests Add to marked items
DOI	10.1007/978-3-540-73001-9_45
Book Series	Lecture Notes in Computer Science
Volume	Volume 4497/2007
Book	Computation and Logic in the Real World
Authors	Oleg V. Kudinov and Victor L. Selivanov
Subject Collection	Computer Science
Text	PDF (410 kb)
<hr/>	
 37.	Book Chapter Short 2-Move Undeniable Signatures Add to marked items
Category	Signatures and Lightweight Cryptography
DOI	10.1007/11958239_2
Book Series	Lecture Notes in Computer Science
Volume	Volume 4341/2006
Book	Progress in Cryptology - VIETCRYPT 2006
Authors	Jean Monnerat and Serge Vaudenay
Subject Collection	Computer Science
Abstract	...we offer a solution to this problem in the context of undeniable signatures with interactive verification protocols

by proposing a way
to achieve these
protocols...

Text

PDF (596 kb)

37 Results First | 1-10 | 11-20 | 21-30 | **31-37** | Next

Frequently asked questions | General information on journals and books | Send
feedback | Impressum

© Springer. Part of Springer Science+Business Media

Privacy, Disclaimer, Terms and Conditions, © Copyright Information

Remote Address: 151.207.242.4 • Server: mpweb18

HTTP User Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; InfoPath.1; .NET CLR 2.0.50621)

Dialog DataStar[options](#)[logoff](#)[tracker](#)[feedback](#)[help](#)

Advanced Search: Examiners' Electronic Digest Database (EEDD)

[limit](#)

Search history:

No.	Database	Search term	Results	
CP		[Clipboard]	0	-
1	EEDD	group ADJ homomorphism	0	-
2	EEDD	homomorphism	0	-
3	EEDD	abelian AND hash	0	-
4	EEDD	abelian AND signature	0	-

[hide](#) | [delete all search steps...](#) | [delete individual search steps...](#)Enter your search term(s): [Search tips](#)[whole document](#)

To restrict search by date, use the limit button.

[search](#)☐ Documents available in fulltext

Select special search terms from the following list(s):

Document type

[Top](#) - [News & FAQs](#) - [Dialog](#)

© 2007 Dialog

[Home](#) | [Login](#) | [Logout](#) | [Access Information](#) | [Alerts](#) | [Purchase Hits](#)

Welcome United States Patent and Trademark Office

☐ Search Results[BROWSE](#)[SEARCH](#)[IEEE XPLORE GUIDE](#)

Results for "(['group homomorphism' <and> signature)<in>metadata)"

Your search matched 0 of 1692897 documents.

A maximum of 100 results are displayed, 25 to a page, sorted by Relevance in Descending order.



» Search Options

[View Session History](#)[New Search](#)

» Key

IEEE JNL	IEEE Journal or Magazine
IET JNL	IET Journal or Magazine
IEEE CNF	IEEE Conference Proceeding
IET CNF	IET Conference Proceeding
IEEE STD	IEEE Standard

Modify Search

(['group homomorphism' <and> signature)<in>metadata)

[Search](#) >☐ Check to search only within this results set

Display Format:



Citation



Citation & Abstract

IEEE/IET

Books

Educational Courses

IEEE/IET journals, transactions, letters, magazines, conference proceedings, and standards.

[view selected items](#)[Select All](#) [Deselect All](#)

No results were found.

Please edit your search criteria and try again. Refer to the Help pages if you need assistance revising your search

[Help](#) [Contact](#)[Copy](#)Indexed by
 Inspect


[Home](#) | [Login](#) | [Logout](#) | [Access Information](#) | [Alerts](#) | [Purchase History](#)

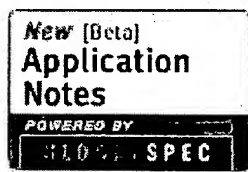
Welcome United States Patent and Trademark Office

[Search Results](#)[BROWSE](#)[SEARCH](#)[IEEE XPLORE GUIDE](#)

Results for "((homomorphism <and> signature)<in>metadata)"

Your search matched 3 of 1692897 documents.

A maximum of 100 results are displayed, 25 to a page, sorted by Relevance in Descending order.

[» Search Options](#)[View Session History](#)[New Search](#)[» Key](#)

IEEE JNL	IEEE Journal or Magazine
IET JNL	IET Journal or Magazine
IEEE CNF	IEEE Conference Proceeding
IET CNF	IET Conference Proceeding
IEEE STD	IEEE Standard

Modify Search

((homomorphism <and> signature)<in>metadata)

[Search](#)☐ Check to search only within this results set

Display Format:



Citation



Citation & Abstract

[IEEE/IET](#)[Books](#)[Educational Courses](#)

IEEE/IET journals, transactions, letters, magazines, conference proceedings, and standards.

[view selected items](#)[Select All](#) [Deselect All](#)

1. **Signature scheme based on discrete logarithm without using one-way hash-function**
Yeun, C.Y.; Mitchell, C.J.; Ng, S.L.;
[Electronics Letters](#)
Volume 34, [Issue 24](#), 26 Nov. 1998 Page(s):2329 - 2330
[AbstractPlus](#) | Full Text: [PDF\(236 KB\)](#) IET JNL
2. **Signature scheme based on discrete logarithm without using one-way hash function**
Zuhua Shao;
[Electronics Letters](#)
Volume 34, [Issue 11](#), 28 May 1998 Page(s):1079 - 1080
[AbstractPlus](#) | Full Text: [PDF\(248 KB\)](#) IET JNL
3. **Parsing languages by pattern matching**
Rus, T.;
[Software Engineering, IEEE Transactions on](#)
Volume 14, [Issue 4](#), Apr 1988 Page(s):498 - 511
Digital Object Identifier 10.1109/32.4672
[AbstractPlus](#) | Full Text: [PDF\(1284 KB\)](#) IEEE JNL
[Rights and Permissions](#)

[Help](#) [Contact](#)[© Copy](#)

Indexed by
 Inspec